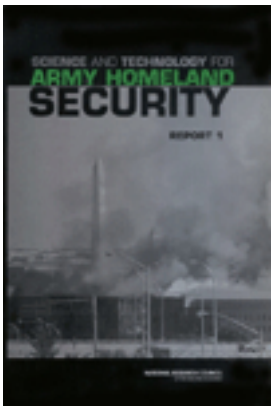
Free Executive Summary



Science and Technology for Army Homeland Security: Report 1

Committee on Army Science and Technology for Homeland Defense, National Research Council

ISBN: 0-309-08701-5, 184 pages, 6 x 9, paperback (2003)

The confluence of the September 11, 2001 terrorist attack and the U.S. Army's historic role to support civil authorities has resulted in substantial new challenges for the Army. To help meet these challenges, the Assistant Secretary of the Army for Research and Technology requested the National Research Council (NRC) carry out a series of studies on how science and technology could assist the Army prepare for its role in homeland security (HLS). The NRC's Board on Army Science and Technology formed the Committee on Army Science and Technology for Homeland Security to accomplish that assignment. The Committee was asked to review relevant literature and activities, determine areas of emphasis for Army S&T in support of counter terrorism and anti-terrorism, and recommend high-payoff technologies to help the Army fulfill its mission.

The Department of Defense Counter-Terrorism Technology Task Force identified four operational areas in reviewing technical proposals for HLS operations: indications and warning; denial and survivability; recovery and consequence management; and attribution and retaliation. The study sponsor asked the Committee to use these four areas as the basis for its assessment of the science and technology (S&T) that will be important for the Army's HLS role. Overall, the Committee found that:- There is potential for substantial synergy between S&T work carried out by the Army for its HLS responsibilities and the development of the next generation Army, the Objective Force.- The Army National Guard (ARNG) is critical to the success of the Army's HLS efforts.

Executive Summary

The U.S. Army is facing a challenge. At the same time that it launches a transformation toward the futuristic Objective Force, the centuries-old requirement to support civil authorities has been brought to the fore by the terrorist attacks of September 11, 2001. As the Army prepares for its still-evolving role in homeland security (HLS), the National Research Council was requested to establish a study committee under the Board on Army Science and Technology to advise the Army on how science and technology (S&T) could assist in the conduct of HLS. This is the first report from the committee.

This executive summary follows the same organization as the report. The section on background abstracts Chapter 1, where the context for the HLS mission is developed. The remainder of the summary addresses the technologies required over the four operational areas identified by the sponsor:

- Indications and warning,
- Denial and survivability,
- Recovery and consequence management, and
- Attribution and retaliation.

The technologies are displayed in tabular format in Chapters 2-5. Such a format provides the best way to understand the technologies the committee believes are important. A summary table depicting high-payoff technologies is provided at the end of this executive summary and in Chapter 6.

The main observations of this report are as follows:

- The S&T required by the Army for HLS need not be unique. The S&T work already being done for the Objective Force could provide much of the technology needed for HLS. In fact, if approached properly, the HLS effort not only can advance the S&T needed for the Objective Force, but also can assist in developing tactics, techniques, and procedures.
- The Army National Guard is critical to the success of the Army's efforts in HLS.

BACKGROUND

Homeland Security Requirements

While the operational framework[1] for combating terrorism on U.S. soil is still emerging, it is clear that this framework will be national in scope and based on cooperation. Although all disasters—either manmade or natural—are local, any disaster of great magnitude will require close cooperation among federal, state, and local governments. In case of a terrorist attack, the wide-ranging capabilities of our armed forces will most certainly be called on. The Army will have to cooperate with civilian emergency responders in order to save lives and mitigate damage. The Army's notional plan for HLS separates high-intensity homeland defense scenarios from lower-intensity civil support scenarios.

The military is not the only community seeking to learn from the events of September 11. The committee became aware of ongoing efforts in the civil sector to develop equipment for civilian emergency responders. This commercially developed equipment might have great applicability for the Army, but there does not appear to be a mechanism for integrating the research being done in the civilian community with that being done in the military community.[2]

Recommendation. The Army should encourage better coordination of the disparate homeland security science and technology efforts.

Recommendation. The Army should facilitate technology transfer in order to allow the private sector and other government agencies to exploit the homeland security technologies it develops.

---

[1]Operational framework refers to a plan that the Army would use to conduct whatever operations may be necessary in response to a terrorist attack.

[2]The Department of Homeland Security will include a Directorate of Science and Technology headed by an Under Secretary for Science and Technology. The Under Secretary will advise the Secretary on R&D efforts, priorities, goals, objectives, and policies. This might be an ideal site for the integration of civil and military research.

The Army

The Army is organized in three parts: the active Army, the Army National Guard (ARNG), and the Army Reserve. The committee believes that the ARNG will be most involved in HLS events, at least initially, because (1) it is under local (state) command, (2) it is usually closest geographically to probable sites for terrorist attacks, and (3) it is not limited in its law enforcement roles.

Equipment for the ARNG is based on its wartime mission, not its response to civil emergencies. Equipment requirements are established in the U.S. Army Training and Doctrine Command, where the ARNG has not had sufficient representation to make its needs known. Given the increased emphasis on HLS, it appeared to the committee that the ARNG should play a more significant role in determining what its HLS equipment should be.

Recommendation. The Army National Guard's homeland security role must be considered in the development of the Army Science and Technology Master Plan, and resources for these requirements applied as appropriate in developing the Department of the Army Master Priority List.

Link to the Objective Force

While the Army has a long history of providing support to civil authorities, the quest for the Objective Force has great significance for the Army's future. This Army of the future is envisioned to be "more strategically responsive, deployable, agile, versatile, lethal, survivable, and sustainable across the entire spectrum of military operations from major theater war through countering terrorism to Homeland Security" (U.S. Army, 2002).

The modernization strategy that is being used to bring the Objective Force to rapid fruition envisions the acceleration of S&T (U.S. Army, 2002). While many of the Objective Force technologies are directly applicable to the Army's newly energized homeland responsibilities, it may be necessary to modify or adapt specific technologies to serve a dual purpose. In addition, some new capabilities will be needed. The committee believes that if this process is accomplished thoughtfully and flexibly, there are great opportunities for cost-effective procurements, economies of scale, and an ability to accomplish both missions successfully.

Recommendation. To optimize current science and technology efforts, the Army should take advantage of potential transferability between technologies for homeland security and those for the Objective Force.

As the committee became more familiar with civilian first responder requirements, an interesting parallel began to emerge between responding to a domestic

terrorist attack in close cooperation with local authorities and fighting a war in close cooperation with allies and coalitions of allies. In both situations, the Army will be working with groups who have different equipment, different cultures, different operational languages, etc. The requirement to create force packages tailored for particular incidents and to establish interoperable situational awareness and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) will be overriding.

Recommendation. The Army should investigate the technologies necessary to put together on the fly the force packages necessary to meet the requirements of both homeland security and the highly deployable Objective Force.

Recommendation. Given the time lag associated with training personnel and leadership to use new technology, now is the time to start dealing with these issues in the context of homeland security, so that they are well honed by the time the Objective Force is fielded.

INDICATIONS AND WARNING

Indications and warning (I and W) generally refers to the events leading up to an attack. Much of this is the province of the intelligence community. Since the Army will have a significant role in responding to the use of weapons of mass destruction (WMD), the committee focused in this portion of the study on the physical detection of explosives (nuclear and conventional), radioisotopes, chemical agents, and biological agents and on the identification of related cross-cutting S&T.

Traditional Imaging Sensors

The advanced, high-performance imaging systems that infuse all aspects of national security and defense also have relevance for HLS. High-performance sensors, which image in a broad range of spectral bands, are a high priority for numerous theater and national missile defense platforms. The Department of Defense (DoD) in general and the Army have broad programs in this area.

Recommendation. It is critically important that all sensors not only be well characterized at the point of purchase but also be regularly rechecked by competent technicians. Software used to integrate disparate sensors should be well documented and checked against standardized problems.

Chemical Agents

Chemical agents are typically released into the atmosphere, where they form toxic clouds that are moved by atmospheric winds or by ventilation systems. The most desirable situation would be to detect these agents before they

are released into the atmosphere. For weaponized agents this will be difficult because of problems with sensitivity and false alarms when operating in realistic dirty environments.

Biological Agents

The point detection of biological agents is qualitatively different from that of chemical agents. Compared with chemical agents, many orders of magnitude less of biological agent are required to incapacitate an individual. This means that there may be substantially less material to detect. A typical biodetection system involves a cueing, detection, discrimination, and identification sequence. Unlike chemical agents, live biological agents may replicate themselves in the infected population to a detectable level, but only after their release. Replication of infectious agents in the population may also contribute to secondary spread of the disease.

Nuclear Materials

In the case of nuclear weapons, the primary fissionable isotopes of interest are uranium-235, plutonium-239, and uranium-233. In most cases detectors are effective only if they are relatively close to the source of radiation. For example, the signature from a plutonium weapon's spontaneous decay processes will be gamma rays and neutrons. Assuming scattering but no neutron capture between the weapon and the detector, the weapon neutron flux from spontaneous fission will equal the background neutron flux at about 15 meters from the weapon, making detection at a distance problematic. All of the nuclear materials detectors mentioned in the report have relatively short detection ranges and are best suited for choke points or portal geometries or where there is good intelligence on where the material is located.

Conventional Explosives

The majority of terrorist attacks against U.S. forces, facilities, and citizens have involved the use of conventional explosives. The detection and tracking of such explosives is therefore extremely important. The vapor-phase detection of a modern explosive will be possible only if there are detectors in close proximity to the explosive or if there is a very substantial concentration of explosive vapors at a distance from the explosive.

Army weapons and explosives in transit or in storage can be attractive targets for theft or diversion by terrorists. On a broader scale, it would be in the interest of the United States if international protocols were established that called for the insertion of detection markers and identification taggants, worldwide, into all legitimately manufactured explosives to assist both detection and forensic analysis.

Recommendation. An international convention requiring the incorporation of detection markers and identification taggants should be sought.

Techniques to detect packaged dangerous materials are for the most part lacking. The committee learned that such detection is an extremely difficult problem even when the detector can be placed next to the package. New and perhaps radically different approaches will be required. A distributed network could involve fixed sensors and mobile sensors deployed on various platforms including autonomous unmanned air, space, ground, and underwater vehicles. This option opens up substantial opportunities for the investment of Army S&T resources because the S&T involved is more broadly applicable to the Army than just nuclear weapons detection or chemical and biological agent detection.

Recommendation. The Army should ensure from the outset that the necessary interrelationships among the sensor networks and the broader intelligence collection activity are established and maintained as a coherent undertaking.

Recommendation. Army science and technology should aggressively seek out and invest in those cross-cutting sciences and technologies that will benefit both the Objective Force and the homeland security requirement to detect weapons of mass destruction.

DENIAL AND SURVIVABILITY

The principal element of successful denial is good security, including both physical security and cybersecurity. Denial of an attack refers to measures taken to prevent or otherwise thwart an intended terrorist attack, whether by preventing access using, for example, guards or barriers or by other means of interception (e.g., explosive detection and electronic surveillance). Survivability, in contrast, refers to measures taken to mitigate the effects of an attack by such means as structural hardening, protecting personnel, and duplicate resources. Survivability also includes the ability to absorb an attack with acceptable damage and casualties, redundancies that enable continued function after an attack, mitigation of the effects of the attack, and preparations that plan for operation afterward.

Recommendation. To gather valuable and perishable medical and other forensic data, the Army should support the establishment of rapid response data-gathering teams to investigate bombing attacks that may occur in the future. The data collected by these teams should be integrated with information from past events and made available to researchers and practitioners in emergency medicine, injury epidemiology, search and rescue, architecture, and engineering.

The fixed infrastructure targets presumed to be of primary interest to the Army are military buildings either inside an installation or standing alone (e.g., barracks, office buildings, and command-and-control (C2) centers), bridges, tunnels, and dams, as well as special facilities such as nuclear power plants and critical Department of Defense (DoD)/Army assets (e.g., ports and airfields). Infrastructure targets also can include those that are primarily "cyber"—computer networks, communication systems, and C2 systems or supervisory control and data acquisition (SCADA) systems for base power grids and water systems.

Physical Security

The technology needs for physical security are very broad. Explosive threats against conventional buildings of direct interest to the Army may range from small 1- or 2-pound explosives packaged in letter bombs or pipe bombs, to hundreds of pounds of explosives contained in cars, to thousands of pounds of TNT (trinitrotoluene) equivalent charge carried by large trucks, trains, or dockside ships.

Military and conventional buildings are susceptible to chemical, biological, and radiation attacks by terrorists through their heating, ventilation, and air-conditioning (HVAC) systems. The effectiveness of such attacks can be greatly reduced by incorporating building automation systems that can be designed to manage specific threats and scenarios.

Recommendation. The Army should monitor and integrate new heat, ventilation, and air-conditioning technologies developed by the Defense Advanced Research Products Agency and other organizations into building and infrastructure design and retrofit guidelines. These technologies include detection, neutralization, filtration, and active ventilation defenses.

The Technical Support Working Group (TSWG)/Defense Threat Reduction Agency (DTRA) Blast Mitigation for Structures Program is a focused and valuable program of research, testing, engineering analysis, and computational modeling to supplement existing knowledge on blast effects and blast-resistant design and construction. However, the full benefits of the program will be realized only if the results are widely disseminated and necessary improvements implemented.

Blast-hardening technologies and design principles developed by the Army and other DoD components for military purposes are generally relevant for federal force protection and civilian design practice. However, because the knowledge base is incomplete, this information must be adapted and expanded to be more specifically usable by and accessible to civilian architects and engineers.

Recommendation. The Army should continue to survey and evaluate relevant ongoing university research with the objective of identifying and synthesizing technology that could improve the performance of buildings in a

blast environment, and it should also consider inviting universities to participate directly in the research effort.

Information Security and Cyber Issues

The word "cyber" is used in this report to refer to any activities related to the computer and communications (C&C) infrastructure, including information stored and/or transmitted in the systems. Use of this infrastructure is rapidly becoming ubiquitous in all aspects of daily life. The C&C infrastructure can be compromised by several mechanisms, principally these:

- An insider making use of authorized access,
- Unauthorized access via direct tapping into the physical facility,
- Unauthorized access via valid network connections and security flaws in the system, and
- Denial-of-service attacks.

There are three primary objectives of a cyber attack:[3] (1) destroy or change data within the system itself, (2) take control of systems controlled by the C&C system, or (3) deny the user effective use of the system. Future terrorist incidents in the United States might utilize any of these. The best defense is to physically isolate an important network from the public network.

Large organizations are often tempted to custom design their own systems, because they believe their needs are different and that they can achieve greater efficiency by dropping those system elements they do not require, at least at the time of design. For general-purpose systems this is not only a false economy—the design costs are such that because of the rate of change in the field, the organization will soon be left with an out-of-date software design that runs only on out-of-date hardware—but it is also an invitation to security disasters.

Recommendation. The Army should partner with other agencies and the commercial sector to develop and adopt the appropriate tools and protocols for the protection of its own computer and communication systems.

Recommendation. The Army should continue to review its cybersecurity procedures to assure that the best practices from the community are adopted on an ongoing basis.

[3]Attacks by hackers merely to prove their abilities by making annoying but inconsequential changes to the system are not discussed. It should be recognized that many of these hacker attacks are against that part of the network that is designed to be public, that is to say public Web sites. While it is desirable to keep those pages secure against unauthorized change, the level of security that can be applied to nonpublic information is necessarily lower.

The Army must be concerned not only with the survivability of its own systems in the event of an attack but also with the survivability of systems over which it has no or little control prior to the attack—or even, perhaps, after the attack—since if it is called on to provide support, it will need to establish links between its units and civilian responders.

Recommendation. Whether through the Army National Guard or active or reserve Army units, the Army should play a major role in providing emergency command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) in the event of a major natural or terrorism disaster because it has both the skill set and the equipment to provide such services in hostile environments.

Recommendation. Equipment and trained personnel should be available to provide vital information and communications for interoperable command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) in the case that civilian systems are seriously impaired in an emergency event.

CONSEQUENCE MANAGEMENT AND RECOVERY

Generally, recovery is viewed as a local and private sector responsibility. However, in the case of terrorist acts using WMD or significant cyberattacks on the nation's critical infrastructure, the damage may exceed the capacity of local agencies and the private sector that owns and operates the critical infrastructure. Consequence management is more than just minimizing the damage; it also involves rescue of and aid to injured victims and the restoration of essential services.

Interoperable C4ISR system

The architecture and technology needed for a HLS C4ISR system is compatible with the Army's framework for developing and fielding the Objective Force. However, Objective Force C4ISR systems will need to be adapted for this different mission and different challenges.

Recommendation. To facilitate the development and fielding of an integrated command-and-control system for homeland security, the Army should initiate or continue research that permits the earliest possible fielding of deployable communications packages equipped with universal multiplexer capability to facilitate C2 across the vast, and disparate, array of agencies that will respond to incidents and events.

Rapid Event Assessment of Physical Damage, Casualties, and Contamination

A necessary condition to conduct recovery and consequence management (R and CM) activities is an assessment of the situation. The Family of Integrated Operational Pictures (FIOP) is designed to meet the needs of the war fighter. However, it could be extended to the HLS mission. A number of sensors exist that can assist with a real-time situational assessment. Overhead imagery from satellites and high-endurance unmanned aerial vehicles (UAVs) can build an optical and infrared picture of physical damage. They can also use measurement and signal intelligence to determine WMD contamination. Reports and images from multiple sensors do not, by themselves, build the situational awareness and operational picture needed to conduct effective operations. The sensor pictures and reports need to be analyzed and depicted on a common grid and shared with the R and CM forces. Finally, a family of models that can predict physical damage, contamination, and casualties can play an important role in the HLS mission.

Recommendation. The Army should conduct research on processes and systems to facilitate the event assessment process. It should support high-priority research such as sensor networking and fusion to merge reports from disparate sensors into a common picture.

Force Protection

The forces employed for large-scale R and CM activities need to be protected for sustained operations. Individual protection suits and inoculations are necessary to sustain operations in WMD conditions. The Army, through its Soldier and Biological Chemical Command (SBCCOM), continues to lead in the development of individual and collective protection technologies. Mobile collective protection facilities are necessary for long-term R and CM activities. The Army is currently developing a new family of deployable collective shelters that can be used by forces engaged in the HLS mission. The primary responsibility for the development of vaccines and medical countermeasures to protect against biological agents rests outside the Army in the Department of Health and Human Services and the Centers for Disease Control. However, the expertise in Army laboratories is essential to progress in this area.

Recommendation. The Army's research and development across the spectrum of technologies needed for individual and collective protection against the effects of weapons of mass destruction for the Army and civilian emergency responders should be continued.

Treatment of Mass Casualties

It is likely that mass casualties will result from the use of WMD and high explosives. A mass casualty incident is one in which there are not enough resources for casualty management. In addition, triage takes on an entirely new aspect, one closely resembling the wartime rules of engagement. Where the cause of injury is suspected to be a chemical agent, toxin, or toxic industrial chemical, the responders must be able to identify the agent and determine the concentration. Methods for field assessment of biological hazards are also employed at this phase of the operation. While it is essential that the military be able to interface with civilian HLS activities as needed, some aspects of military capability may not perfectly match HLS needs.

Recommendation. The Army should expand its research in the area of triage, tracking, and treatment of mass casualties.

Recommendation. The Army should ensure development of individual triage assessment for mass casualties from events involving weapons of mass destruction.

Recommendation. The Army should ensure the development of a process to leverage information technology to effectively conduct mass casualty triage, tracking, and treatment following such an event. The process development should incorporate (1) remote decision support systems that can be integrated with civilian systems and (2) a tracking system.

Containment and Decontamination of the Effects of WMD

There is not much experience in wide-area decontamination in the aftermath of chemical, biological, and radiological/nuclear weapons attacks. Even with a correct assessment of the levels of contamination, there are few tools and techniques available for decontamination. Decontamination will probably be accomplished in stages, and it is likely that the Army will be involved in early remediation of WMD events.

Recommendation. Army science and technology should concentrate on the further development of a process to plan and implement remediation and decontamination for chemical, biological, radiological, and nuclear events. This process must be capable of being conducted in real time based on limited information.

Recommendation. Army science and technology should concentrate on the further development of decontamination solutions for chemical, biological, radiological, nuclear, or even large explosive events weapons.

ATTRIBUTION AND RETRIBUTION

In general, attribution is assigning a cause or source to an act or event. In the context of this report, it is the identification of individuals or organizations that are responsible for direct or indirect acts of terrorism and sabotage directed against the United States, its territories, and vital national interests. Retaliation is action taken in return for an injury or offense and to deter future attacks.

While the committee has no recommendations for attribution—leaving that to nonmilitary agents—the Army's role in retaliation runs the gamut from simple military/law enforcement coordination, when appropriate, to full-blown remote operations overseas, where the Army may be assigned primary ground retaliation responsibility as part of a Joint Task Force. Since this role is primary to the Army, the committee believes there are some enabling technologies that should receive very high priority and deserve S&T investment.

Operational Area and the Army Role

Operations in urban environments and in the presence of noncombatants will probably be common. The ability to move quickly in a crowded city swarming with civilians and hiding some terrorist cells is an extremely complicated task. This problem was clearly demonstrated in Somalia. The Army must be able to move personnel quickly, through or over busy streets. The committee feels that exoskeleton technology significantly increases the running and jumping capability of the individual soldier. Likewise, there is a need for small, armor-plated, light transport vehicles, ground and helicopter, to move forces as needed in this environment. Additionally, a capability is needed for clearing obstacles in the streets and alleyways.

Technology Focus Areas

One key aspect of survivability is signature reduction of our forces across the spectrum—radio frequency (RF), electro-optical, infrared, radar, acoustic, etc. Additionally, enhanced armor protection is of critical importance in the Objective Force Warrior program. Fire support plays a critical role in all combat operations. The vast majority of current fire support systems were not developed specifically for urban warfare, where precision and lethality (or nonlethality) can determine the outcome of an operation. Even relatively small errors can be devastating in terms of collateral damage or innocent civilians killed.

Recommendation. The Army should continue and enhance current research and development to focus on mobility operations in the urban environment, to include exploration of small, mobile armored carriers for use in urban environments and mini-breachers to clear streets and alleyways.

There is no good system for achieving situational awareness in an urban environment. This is due in part to the extremely complex RF propagation environment in this setting, coupled with the high-resolution accuracy needed to track a soldier in a specific room or building. A comprehensive situational awareness system building on the current Land Warrior system and linking the individual soldier to on-the-body, local, and remote sensor systems and information databases is necessary.

Recommendation. The Army should modify current systems or develop new systems, along with appropriate munitions, that are specifically designed for extremely precise fire support in urban environments.

Recommendation. The Army should make technologies such as the situational awareness Blue Force Tracking program and the health monitoring system available to the Department of Homeland Security, which will consider whether or not they can be adapted for civilian use.

Locating and tracking small terrorist cells in a rural environment is a very difficult task, particularly when the terrorist attempts to blend into the environment. Several advanced technologies may help the war fighter locate terrorists in this environment. However, there may well be a physical limitation to detector capability.

Recommendation. The Army should continue to develop a robust soldier situational awareness system begun in Land Warrior that provides a real-time, fused information system.

Recommendation. The Army should adopt a tiered approach to the problem of terrorist cell tracking and surveillance in the urban environment and in rugged terrain, first increasing sensor sensitivity, then networking and fusing sensors, and, finally, fusing information from disparate sources.

The committee believes that defense of the homeland is the military's top priority and that the Army will play a significant role in this action. Science and technology can and will assist the Army in this role.

Recommendation. The Army should focus its funding and research efforts on the high-payoff technologies shown in summary Table ES-1.

TABLE ES-1 High-Payoff Technologies

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
Chapter 2	Indications and Warning Technologies		
Perimeter defense and warning	HgCdTe imaging LWIR arrays to fabricate high-performance detector arrays.[c]	R	H, O, C
	Uncooled bolometer arrays utilizing temperature-dependent dielectric constants and operating at room temperature.[c]	R, N	H, O, C
	GaAs quantum well arrays; a type of extrinsic photoconductor in which the bound electrons reside inside the quantum wells instead of on dopant ions.[c]	R, N	H, O, C
	GaN UV detectors for solar blind applications.[d]	F	H, O, C
Biological agent detection	DNA microarrays that can monitor thousands of genes simultaneously.	F	H, O, C
	Combinatorial peptides using massive libraries for screening.	F	H, O, C
	Raman scattering; matches observed Raman spectra against a library of predetermined signatures.[e]	N, F	H, O, C
Vapor-phase explosive detectors	Chemical resistors that detect at the parts per billion level. Must be close to explosive or chemical, needs improved SNR.[f,g]	N	H, O, C
	Fluorescent polymers that detect at parts per trillion level (in principle). Must be close to explosive or chemical, needs improved SNR. Demonstrated at parts per billion in reliable system.[h]	R, N	H, O, C
	Surface-enhanced Raman spectroscopy that detects at parts per billion. Portable, must be close to explosive.[h]	N, F	H, O, C
	Immunoassay (biosensors) that detects parts per billion. Must be close to explosive. Potential for increased sensitivity.[h]	N, F	H, O, C

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
Bulk explosive detection	Nuclear quadrupole magnetic resonance (NQR). Low SNR, must be close to explosive, does not require magnets. Produces RF signals characteristic of particular explosives.[g,i]	R, N	H, O, C
	Millimeter-wave radiometry. Potential to provide radiometric images of objects (e.g., explosives) under clothing. [g,j]	N	H, O, C
Cross-cutting detection and tracking	Sensor networking—gathers data from a wide variety of spatially distributed sensors.	N, F	H, O, C
	Sensor fusion—intelligently combines, correlates, and interprets data from distributed sensors.	N, F	H, O, C
	Anomaly detection—examines data from networked sensors to discover patterns, unusual behavior, etc.	N, F	H, O, C
	Surveillance platforms (UAVs, UGVs, UUVs)—small autonomous vehicles for carrying sensor payloads as part of distributed sensor network.	R, F	H, O, C
Cross-cutting perimeter surveillance	IR, RF, acoustic, seismic, etc. techniques that monitor for intrusion into predetermined spaces (encampments, facilities, borders, etc.).	R, N	H, O, C
Cross-cutting capability in miniaturized systems	MEMS—methods for integration of many technologies into microsensors using electronic fabrication technologies.	R, F	H, O, C
	Active-passive sensor suites—suites of lasers and detectors that can query and image as well as perform spectroscopic measurements.	N, F	H, O, C
	Nanofabrication techniques—fabrication of sensing systems at the atomic level.	F	H, O, C

Continues

TABLE ES-1 Continued

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
Chapter 3	Denial and Survivability Technologies		
Perimeter control	X-ray assessment, swimming sensors for rapid detection of LVBs.	N, F	H, O
	Unattended sensor networks, advanced power sources, C2 and secure communication, low-power sensing elements for deployable perimeter control system.	N, F	H, O
	C2 and secure communications, situational awareness tools, area sensors for mobile perimeter system.	F	H, O
Building and facility access control	Smart ID with bioinformation, ID tracking with area authorization, iris ID, liveness tests, auto DNA ID for automatic, high-confidence access control.	F	H, O, C
Structural blast resistance	Prediction of blast and impact loads on and in buildings, bridges, dams, etc.	N, F	H, O, C
	Connection details for steel and concrete structures (new and retrofit construction) to upgrade current approaches for dynamic environments and material behavior.	N	H, O, C
	Methodology to prevent/evaluate potential for progressive collapse.	N (+ university, industry)[k]	H, O, C
	Blast-resistant window concepts, including new glazing-to-frame connections.	N	H, O, C
	Blast-resistant tempered and laminated glass (stiffness, strength enhancement, ductility).	F	H, C
	First-principles analysis techniques to supplement experimental databases for design of windows and structural component retrofits.	N	H, O, C
	Software to include new test and analysis data and techniques for design and retrofit of structures in blast environments.	R, N	H, O, C

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
	Integration of performance standards with building codes from a multihazard perspective.	N, F	H, O, C
Cybersecurity	IP version 6 to provide ad hoc mobile C&C networks to rapidly reconfigure systems.	N	H, O, C
	Technologies to avoid enemy intrusions, guarantee functionality.	F	H, O
	Technologies to provide alternative C&C after a disaster.	N	H, O
	IP version 6 for networks, universal radio, etc. to allow the Army systems to interoperate with other emergency services.	N	H, O
Chapter 4	Recovery and Consequence Management Technologies		
Command and control	Adaptive integrated multiplexer systems to integrate communications between multiple agencies.	N	H, O, C
	Mobile local broadband networks to pass imagery and communications.	N, F	H, C
	Blue Force Tracking to determine the location of operational personnel and assets from multiple agencies.	N, F	H, O, C
Planning	Decision support aids such as those in the Agile Commander ATD to enhance real-time planning among multiple agencies.	N	H, O
Event assessment	Family of interoperable operational pictures displays that can be shared by operational planners and implementers.	N, F	H, O, C
	Land mobile robotics that can breach obstacles to implant sensors.	R, N	H, O, C
	Sensor networking and fusion to integrate multiple sensors into a common picture.	N, F	H, O, C

Continues

TABLE ES-1 Continued

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
	Real-time damage and contamination modeling to provide attack assessments based on the reports of fused sensor data.	N, F	H, O, C
Force protection	Development of improved protective mask filters and service-life indicators.	R, N	H, O, C
	Development of semipermeable membranes and self-detoxifying material for protective suits.	N	H, O, C
	Vaccine development for protection against biological agents.	N, F	H, O, C
Medical response	Chemical, biological, and radiological triage assessment cards providing C4ISR integration of data, decontamination of the patients and material, tracking of the patients, physical evidence, clothing; chain of custody.	R, N	H, O, C
	C4ISR; on-demand access to expert's network, scenario modeling/procedures to provide remote expert support for the on-site medical personnel; on-demand linkage to medical and scientific information systems, experts, and laboratories.	R, N	H, O, C
	Field-deployable diagnostic, life-support, and emergency surgical systems that can be easily and rapidly deployed; that are resistant to vibration, low environmental quality, and electromagnetic interference; and that can be operated efficiently in the presence of chemical, biological or radiological residuals.	R, N, F	H, O, C
	Field-deployable rapid-assay devices; dynamic meteorologic models of CBRN threats to provide the first responder an assessment of agents and risks for staff and patients; assessment of ongoing environmental risks.	R, N	H, O, C

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
	Scenario development software based on physiologic and biochemical response to agents.	R, N	H, O
	Hemorrhage, neurological, and respiration stabilizing devices and technologies with a long shelf-life, rapid-acting agents.	R, N	H, O, C
	Vaccines and immunologic factors (including therapeutic applications), counteragents for chemical, biological, and radiological exposure with a long shelf-life, rapid-acting agents.	R, N, F	H, O
	Distributed learning platforms with AI and decision-assisting tools for CBRNE.	R, N, F	H, O
Remediation and decontamination	Development of a process to plan and implement remediation and decontamination for chemical, biological, radiological, and nuclear events.	N	H, C
	Further development and assessment of solutions to clean up chemical and biological contamination.	R, N, F	H, C
Chapter 5	Attribution and Retaliation Technologies		
Detect traffic/ activity abnormality in urban and rural locations	Multisensor fusion.	N	H, O
	Data mining techniques.	N	H, O
	Inference algorithms.	N	H, O
	Redeployable UGS.	F	H, O
Locate terror cells in areas of heavy foliage	3-D ultrasensitive lidar.	N	O
Defeat covered and concealed targets in rural environment	3-D ultrasensitive lidar.	N	O
	Multisensor fusion techniques.	N	O

Continues

TABLE ES-1 Continued

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
Locate gunshots in urban environment	Ultrasensitive acoustics triangulation system.	F	H, O, C
Enhanced red force (enemy) location in urban environment	Track deconfliction algorithms.	F	O
Situational awareness	Enhanced blue force (friendly) personnel location in urban environment provided by fused GPS, RF, and dead-reckoning hardware and algorithms.	N	H, O, C
Mobility in remote urban environment	Exoskeleton for soldier platform.	F	O, C
	Light, highly survivable, signature-suppressed troop-carrying helicopter.	F	O, C
	Mobile, small-scale robotic breachers for clearing alleys, etc. in urban environment.	N, F	O, C
Remote operations	Reduced usage of signature-producing technologies.	N	H, O
	Advanced composites for lightweight armor protection.	F	H, O, C
	Advanced composites for enhanced vehicle mine protection.	F	H, O, C
	Advanced health and wound monitoring system that integrates blood pressure, heart rate, body temperature, skin penetration sensors.	N, F	H, O, C
Munitions and delivery systems designed for remote urban combat	Nonlethal munitions to include acoustic systems.	N, F	H, O, C
	PSYOP products.	N	O
	UAVs and UGVs designed for urban fire support.	N	H, O, C

Function	Technology	Availability[a] (R, N, F)	Multiuse[b] (H, O, C)
Precision insertion and targeting for warheads	Advanced propellants.	N, F	O
	Improved warhead design,	N, F	O

NOTE: AI, artificial intelligence; ATD, Advanced Technology Demonstration; CBRN, chemical, biological, radiological, and nuclear; CBRNE, chemical, biological, radiological, nuclear, and high explosive; C&C, computers and communication; C2, command and control; DARPA, Defense Advanced Research Projects Agency; EO, electro-optical; FOLPEN, foliage penetration; GPS, Global Positioning System; ID, identification; IP, Internet protocol; IR, infrared; lidar, light detection and ranging; LVB, large vehicle bomb; LWIR, long-wave infrared; MEMS, microelectromechanical systems; NSA, National Security Agency; PSYOP, psychological operations; RF, radio frequency; SNR, signal-to-noise ratio; UAV, unmanned air vehicle; UGS, unattended ground sensor; UGV, unmanned ground vehicle; UUV, unmanned underwater vehicle; UV, ultraviolet; 3-D, three-dimensional.

[a]Availability: R, ready (TRL 8-9); N, near-term (TRL 4-7); F, far-term (TRL 1-3).

[b]Multiuse: H, Army homeland security; O, Objective Force; C, civilian (first responders and others).

[c]Westervelt et al. (1991).

[d]DARPA (2002a,b).

[e]NATIBO (2001).

[f]Lewis et al. (1997).

[g]Bruschini and Gros (1997).

[h]Ward et al. (2001).

[i]U.S. Navy (2002).

[j]NRC (1996).

[k]Participation by universities and industry should be sought, because their technology, understanding, experience, and capabilities in this area are advanced, their databases are useful, and they would provide new insight and information to the program and shorten the time frame for development.

REFERENCES

Bruschini, C., and B. Gros. 1997. A Survey of Current Sensor Technology Research for the Detection of Landmines. Available online at <http//diwww.epfl.ch/lami/detec/susdemsurvey.html>. Accessed on September 24, 2002.

DARPA (Defense Advanced Research Projects Agency). 2002a. Semiconductor Ultraviolet Optical Sources (SUVOS) Available online at <http://www.darpa.mil/mto/suvos/index.html>. Accessed on October 2, 2002.

DARPA. 2002b. Solar Blind Detectors. Available online at <http://www.darpa.mil/MTO/SBD/index.html>. Accessed on October 2, 2002.

Lewis, N.S., M.C. Lonergan, E.J. Severin, B.J. Doleman, and R.H. Grubbs. 1997. Array-based vapor sensing using chemically sensitive carbon black-polymer resistors. Pp. 660-670 in Detection and Remediation Technologies for Mines and Minelike Targets II, Proceedings of SPIE, vol. 3079, A.C. Dubey and R.L. Barnard, eds. Bellingham, Wash.: The International Society for Optical Engineering.

NATIBO (North American Technology and Industrial Base Organization). 2001. Biological Detection System Technologies Technology and Industrial Base Study, February, Available online at < http://www.dtic.mil/natibo/>. Accessed on September 23, 2002.

NRC (National Research Council). 1996. Airline Passenger Security Screening: New Technologies and Implementation Issues. Washington, D.C.: National Academies Press.

U.S. Army. 2002. Weapon Systems 2002. Washington, D.C.: Government Printing Office.

U.S. Navy. 2002. Department of the Navy Explosive Detection Equipment-Explosives. Available online at <http://explosivedetection.nfsec.navy.mil/explosives./htm>. Accessed on September 24, 2002.

Ward, K.B., A. Ervin, J.R. Deschamps, and A.W. Kusterbeck. 2001. Force Protection: Explosives Detection Experts Workshop, NRL/MR-MM/6900—01-8564, CDROM. Arlington, Va.: Office of Naval Research.

Westervelt, R., J. Sullivan, and N. Lewis. 1991. Imaging Infra-red Detectors. JASON report number JSR-91-600. McLean, Va.: Mitre Corporation.

SCIENCE AND TECHNOLOGY FOR ARMY HOMELAND SECURITY

REPORT 1

Committee on Army Science and Technology for Homeland Defense
Board on Army Science and Technology
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract/Grant No. DAAD19-02-C-0049, TO 2, between the National Academy of Sciences and the Department of the Army. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organization that provided support for the project.

International Standard Book Number 0-309-08701-5

Cover: The Pentagon burning after being struck by a commercial airliner, September 11, 2001. Courtesy of Reza Marvashti, The Free Lance-Star, Fredericksburg, Virginia.

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Wm. A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON ARMY SCIENCE AND TECHNOLOGY FOR HOMELAND DEFENSE

JOHN W. LYONS, NAE, *Chair,* U.S. Army Research Laboratory (retired), Mount Airy, Maryland
GEORGE BUGLIARELLO, NAE, Polytechnic University, Brooklyn, New York
TIMOTHY COFFEY, University of Maryland, College Park, with joint appointment at National Defense University, Washington, D.C.
STEPHEN W. DREW, NAE, Princeton University, Princeton, New Jersey
MITRA DUTTA, University of Illinois, Chicago
FREDERICK L. FROSTIC, Booz Allen Hamilton, McLean, Virginia
C. WILLIAM GEAR, NAE, NEC Research Institute, Princeton, New Jersey
ARTHUR H. HEUER, NAE, Case Western Reserve University, Cleveland, Ohio
HOWARD S. LEVINE, Weidlinger Associates, Inc., Los Altos, California
JOSEPH P. MACKIN, E-OIR Measurements, Inc., Spotsylvania, Virginia
JACK N. MERRITT, U.S. Army (retired) and Association of the U.S. Army (retired), Arlington, Virginia
THOMAS E. MITCHELL, Gray Hawk Systems, Inc., Alexandria, Virginia
K. DAVID NOKES, Sandia National Laboratories, Albuquerque, New Mexico
DENNIS J. REIMER, U.S. Army (retired) and Memorial Institute for the Prevention of Terrorism, Oklahoma City
EUGENE SEVIN, NAE, Consultant, Lyndhurst, Ohio
ANNETTE L. SOBEL, Sandia National Laboratories, Albuquerque, New Mexico
MICHAEL F. SPIGELMIRE, U.S. Army (retired), Consultant, Destin, Florida

Liaison, Board on Army Science and Technology

DONALD R. KEITH, U.S. Army (retired) and Cypress International (retired), Alexandria, Virginia

National Research Council Staff

MARGARET N. NOVACK, Study Director
JAMES C. MYSKA, Research Associate
TOMEKA N. GILBERT, Senior Project Assistant

Preface

This study is being conducted by the Committee on Army Science and Technology for Homeland Defense of the Board on Army Science and Technology, in the Division on Engineering and Physical Sciences of the National Academies. Sponsored by the Deputy Assistant Secretary of the Army for Research and Technology, the committee will produce a series of reports encompassing possible science and technology in support of the Army's role in homeland security (HLS). The statement of task for this first report is as follows:

> The National Research Council will:
>
> Review relevant literature and activities, such as the National Academies' emerging Science and Technology Program plan and Research Strategy for Combating Terrorism and their work with the interagency Technical Support Working Group (TSWG), reports from the Gilmore Commission and Hart-Rudman Commission, the DoD Counter-Terrorism Technology Task Force (DCT3F) plan, DOD Information Assurance policies and existing military operation and contingency plans to develop an Army context for the enhanced campaign against terrorism.
>
> Determine areas of emphasis for Army S&T in support of counterterrorism (CT) and anti-terrorism (AT). Operational areas the NRC should examine include indications and warning, denial and survivability, recovery and consequence management, and attribution and retaliation.
>
> In the first year, produce a report within nine months from contract award containing findings and recommendations that provide insights for high-payoff technologies.

BACKGROUND OF THE STUDY

The terrorist attacks of September 11, 2001, have forced the nation to consider how to prepare for the defense of the homeland. Terrorism is no longer an item on the evening news, taking place in some distant locale. Terrorism has become a domestic issue. As part of this recognition, the Army requested that the Board on Army Science and Technology (BAST) create a committee to meet over a 3-year period to consider how science and technology might better enable the Army to accomplish its mission in the homeland. It is anticipated that the committee will produce several reports during this period.

COMMITTEE PROCESS

This first report is a broad survey of relevant technologies, written in a relatively short period of time. Because of the scope of the review, the lack of a well-defined operational framework,[1] and the time-sensitive nature of the Army's interest, the committee has determined not to study specific products but rather to consider areas of technologies one level above individual products, processes, or services. In any case it should be noted that it is not the intent of this study to recommend budget actions; the technology assessments are intended to assist the Army in formulating its future technology plans.

The committee began its work by reviewing the literature listed below but found that very little has been said about the Army's role in HLS and the technology needs in support thereof.

- The National Strategy for Homeland Security,
- The Federal Response Plan,
- The National Academies' report *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism,*
- The interagency Technical Support Working Group (TSWG) outputs,
- Reports from the Gilmore Commission and the Hart-Rudman Commission,
- The Department of Defense (DoD) Counter-Terrorism Technology Task Force (DCT3F) plan,
- DoD information assurance policies, and
- Existing military operation and contingency plans.

There are other reports, such as the annual report of the Department of Energy's Chemical/Biological National Security Program (CBNP), that the committee did not review for lack of time but that might provide additional information to the reader.

[1]Operational framework refers to a plan that the Army would use to conduct whatever operation may be necessary in response to a terrorist attack.

In addition to the literature search, the committee requested a series of briefings from the Army to better understand the Army's view of the homeland mission. It also heard from representatives of the National Guard Bureau to understand the role of the Army National Guard. A thorough legal briefing on the limitations of the Posse Comitatus Act facilitated this understanding. Lastly, the committee heard from scientists with expertise in a wide range of technologies in an effort to preview emerging types of equipment.

Even as this report was being prepared, doctrine and policy were being developed. The Department of Homeland Security and the Department of Defense's Northern Command, which are to have the major responsibilities and authorities for homeland security at the national level, are still in the early stages of formation and organization. The actual role that will be played by the Army in homeland security must certainly depend in large measure on the operational assignments Army units will be given in the framework of, or in support of, these overarching organizations. This remains in a state of flux. While, as is indicated in the report, it is anticipated that much of the doctrine will be drawn from existing protocols, the lack of specific doctrine made the study of specific equipment requirements difficult. Therefore the committee assumes certain functional requirements, which are described in Chapter 1.

REPORT ORGANIZATION

The DOD's Defense Counter-Terrorism Technology Task Force (DCT3F), in calling for and reviewing technical proposals in the wake of September 11, used the following taxonomy:

- Indications and warning,
- Denial and survivability,
- Recovery and consequence management, and
- Attribution and retaliation.

The study sponsor chose to make this taxonomy the basis for the committee's tasking document,[2] so the report is organized around these operational areas.

[2]In other documents, the Pentagon has used a different taxonomy but to the same end. For example, the Joint Warfighting Science and Technology Plan uses the following groupings of operational capabilities and subcapabilities:

Prevention	*Protection*	*Response*
Denial	Infrastructure	Attribution
Indications and warnings	Personnel	Consequence management
Deterrence	Facilities	Crisis management
Preemptive strike	Retaliation	

These four areas describe events in a time continuum beginning when intelligence indicates an event may take place and ending when blame can be attributed and appropriate retaliation executed. In Chapters 2 through 5 the committee has divided the four operational areas first into functional capabilities and then into technologies. Because the same technologies may be necessary in more than one of the operational areas, conclusions and recommendations concerning these technologies may appear in more than one chapter. Chapter 6 captures the overarching observations of the committee and Chapter 7 lists the findings, conclusions, and recommendations.

COMMITTEE COMPOSITION

The membership of this committee was intended to contain a broad representation of scientific and technological skill sets that have application to the Army's role in homeland security. These skill sets range from information technologies such as communications, computer sciences, and sensor technologies to materials and civil engineering, with special emphasis on structural hardening and resistance to nuclear and conventional explosive forces. Biosecurity expertise was considered important, as was a thorough understanding of the Army's capabilities. A security clearance was considered essential, as many of the topics that would be of interest to the committee are classified.

The committee worked very hard at its task and is grateful to all those who contributed to the report. Although the report limits itself to a fairly high-indenture level of exploration, the committee is satisfied that it will provide significant assistance to the Army as it moves on to future missions.

John W. Lyons, *Chair*
Committee on Army Science and
Technology for Homeland Defense

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the NRC's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Thomas N. Burnette, Jr., LTG U.S. Army (retired),
Ashton B. Carter, Harvard University,
Anthony Dirienzo, Colsa Corporation,
Ronald O. Harrison, MG, Army National Guard (retired),
J. Jerome Holton, Defense Group Inc.,
Michael R. Ladisch, NAE, Purdue University,
Lewis E. Link, LTG, U.S. Army Corps of Engineers (retired),
John E. Miller, Oracle Corporation,
M. Allan Northrop, Microfluidic Systems, Inc.,
George W. Parshall, NAS, E.I. du Pont de Nemours & Company,
Harvey W. Schadler, NAE, GE Corporate Research and Development, and
Andrew Sessler, NAS, Lawrence Berkeley National Laboratory Center.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recom-

mendations nor did they see the final draft of the report before its release. The review of this report was overseen by Alexander H. Flax, NAE. Appointed by the NRC's Report Review Committee, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Tables, Figures, and Boxes

TABLES

FIGURES

BOXES

Acronyms

2-D	two-dimensional
3-D	three-dimensional
A and R	attribution and retaliation
AMC	Army Materiel Command
ARNG	Army National Guard
ATD	Advanced Technology Demonstration
BCT	brigade combat team
C&C	computer and communications
C2	command and control
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CBR	chemical, biological, and radiological
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high explosive
CM	consequence management
CM and R	consequence management and recovery
CST	civil support team
D and S	denial and survivability
D2PC	Dispersion and Diffusion Puff Calculator
DARPA	Defense Advanced Research Projects Agency

DASA (R&T)	Deputy Assistant Secretary of the Army for Research and Technology
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DTRA	Defense Threat Reduction Agency
EMT	emergency medical team
EPA	Environmental Protection Agency
ESF	emergency support function
FBI	Federal Bureau of Investigation
FCO	federal coordinating officer
FEMA	Federal Emergency Management Agency
FIOP	Family of Integrated Operational Pictures
FRERP	Federal Radiological Emergency Response Plan
GPS	Global Positioning System
HHS	Department of Health and Human Services
HLS	homeland security
HVAC	heating, ventilation, and air conditioning
I and W	indications and warning
ID	identification
IEW	intelligence and early warning
IR	infrared
JIC	Joint Information Center
JOC	Joint Operations Center
LFA	lead federal agency
LVB	large vehicle bomb
LWIR	long-range infrared
NCP	National Oil and Hazardous Substance Pollution Control Plan
NORTHCOM	Northern Command
OPSEC	operational security
OSC	on-site coordinator
PCA	Posse Comitatus Act
PDD	Presidential Decision Directive
ppb	parts per billion

ppm	parts per million
ppt	parts per trillion
R and CM	recovery and consequence management
R&D	research and development
ROC	regional operation center
S&T	science and technology
SBCCOM	U.S. Army Soldier and Biological Chemical Command
SCADA	supervisory control and data acquisition
SNR	signal-to-noise ratio
TRL	technology readiness level
TSWG	Technical Support Working Group
UAV	unmanned air vehicle
UGS	unattended ground sensors
USACE	U.S. Army Corps of Engineers
USAR	U.S. Army Reserve
UV	ultraviolet
VLSTRACK	vapor, liquid, and solid tracking
WMD	weapon(s) of mass destruction